

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN RE APPLICATION OF THE)
UNITED STATES OF AMERICA FOR)
AN ORDER AUTHORIZING THE)
INSTALLATION AND USE OF PEN)
REGISTERS AND TRAP AND)
TRACE DEVICES)

Magistrate No. 18-676

~~UNDER SEAL~~

APPLICATION

The United States of America, moving by and through its undersigned counsel, respectfully submits under seal this *ex parte* application for an order pursuant to 18 U.S.C. §§ 3122 and 3123, authorizing the installation and use of pen registers and trap and trace devices ("pen-trap devices") to record, decode, and/or capture dialing, routing, addressing, and signaling information associated with each communication to or from servers and other infrastructure established by the United States in this investigation. In support of this application, the United States asserts:

I. LEGAL AUTHORITY

1. This is an application¹, made under 18 U.S.C. § 3122(a)(1), for an order under 18 U.S.C. § 3123 authorizing the installation and use of a pen register and a trap and trace device.
2. Such an application must include three elements: (1) "the identity of the attorney for the Government or the State law enforcement or investigative officer making the application"; (2) "the identity of the law enforcement agency conducting the investigation"; and (3) "a

¹ It is not clear that the Pen Register and Trap and Trace Act's prohibition against the "installation" or "use" of a "pen register" or a "trap and trace device" applies to the unique facts presented to the Court here. *See, e.g. Capitol Records Inc. v. Thomas-Rasset*, 2009 WL 1664468, *3 (D. Minn. 2009) ("the Pen Register Act cannot be intended to prevent individuals who receive electronic communications from recording the IP information sent to them. If it did apply in those cases, then the Internet could not function..."). Nonetheless, the United States is applying for a Pen Register and Trap and Trace Order out of an abundance of caution in order to be certain that its conduct will not violate the Act.

certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency." 18 U.S.C. § 3122(b).

3. The undersigned applicant is an "attorney for the government" as defined in Rule 1(b)(1) of the Federal Rules of Criminal Procedure.

4. The law enforcement agency conducting the investigation is the Federal Bureau of Investigation ("FBI").

5. The applicant hereby certifies that the information likely to be obtained by the requested pen-trap devices is relevant to an ongoing criminal investigation being conducted by the FBI.

6. This Court is a "court of competent jurisdiction" under 18 U.S.C. § 3122(a)(2) because it "has jurisdiction over the offense being investigated," 18 U.S.C. § 3127(2)(A)(i).

II. THE RELEVANT FACTS

7. Other than the three elements described above, federal law does not require that an application for an order authorizing the installation and use of a pen-trap device specify any facts. The following information is provided to demonstrate that the order requested falls within this Court's authority to authorize the installation and use of a pen-trap device under 18 U.S.C. § 3123(a)(1).

8. The following is based on information provided by the FBI to me in my official capacity:

A. FBI Investigation of Computer Intrusions

9. The United States is investigating unauthorized computer intrusions being perpetrated by a group known to private cybersecurity investigators as the "Sofacy Group" (also

known as APT28, Sandworm, X-Agent, Pawn Storm, Fancy Bear, and Sednit). According to these cybersecurity researchers, the Sofacy Group is a cyber-espionage group believed to have originated from Russia. Likely operating since 2007, the group is known to target government, military, security organizations, and other targets of intelligence value, through a variety of means. The investigation concerns possible violations of, *inter alia*, § 1030(a)(5)(A)-(C) (causing damage to computers), and § 1030(b) (computer intrusion conspiracy).

10. Relevant to this application, the FBI is investigating routers that Sofacy actors infected with malicious software (or “malware”) and their illegal use of those infected routers to create a “botnet” – a network of other compromised computers. An attacker with access to this botnet would be able to steal and delete files, elevate or escalate privileges, conduct keylogging, and potentially destroy victim files or even render the infected device inoperable.

11. To further the investigation, disrupt the ongoing criminal activity involving the establishment and use of the botnet, and assist in the remediation efforts, the FBI seeks authorization through this pen-trap application to record, decode, and/or capture dialing, routing, addressing, and signaling information (as described in Section II.B below) of communications sent by malware on the infected routers and other devices to the servers and other infrastructure established by the United States in this investigation. Such communications are expected to result from the United States’ contemporaneous seizure of a malicious domain used by the malware pursuant to a separate seizure order.

B. Additional Information Regarding Pen-Trap Devices

12. A “pen register” is “a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or

electronic communication is transmitted.” 18 U.S.C. § 3127(3). A “trap and trace device” is “a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication.” 18 U.S.C. § 3127(4).

13. In the traditional telephone context, pen registers captured the destination phone numbers of outgoing calls, while trap and trace devices captured the phone numbers of incoming calls. Similar principles apply to electronic communications, as described below.

14. The Internet is a global network of computers and other devices. Devices directly connected to the Internet are identified by a unique Internet Protocol (“IP”) address. This number is used to route information between devices. Generally, when one device requests information from a second device, the requesting device specifies its own IP address so that the responding device knows where to send its response.

15. On the Internet, data transferred between devices is not sent as a continuous stream, but rather it is split into discrete packets. Generally, a single communication is sent as a series of data packets. When the packets reach their destination, the receiving device reassembles them into the complete communication. Each packet has two parts: a header with routing and control information, and a payload, which generally contains the content of the transmitted communication.

16. The packet header contains non-content dialing, routing, addressing and signaling information, including IP addresses and port numbers. Both the IP address of the requesting device (the source IP address) and the IP address of the receiving device (the destination IP address) are included in specific fields within the packet header, as are source and destination port numbers.

On the Internet, IP addresses and port numbers function much like telephone numbers and area codes – often both are necessary to route a communication. Sometimes these port numbers identify the type of service that is connected with a communication, such as email or web-browsing, but often they identify a specific device on a private network. In either case, port numbers are used to route data packets either to a specific device or a specific process running on a device. Thus, in both cases, port numbers are used by computers to route data packets to their final destinations.

17. The headers of data packets also contain other dialing, routing, addressing and signaling information. This information includes the transport protocol used (there are several different protocols that govern how data is transferred over networks); the flow label (for the most recent version of the Internet Protocol suite, called IPv6, the flow label helps control the path and order of transmission of packets); and the packet size.

III. GOVERNMENT REQUESTS

18. For the reasons stated above, the United States requests that the Court enter an Order authorizing the installation and use of pen-trap devices to record, decode, and/or capture the dialing, routing, addressing, and signaling information described above for each communication sent by the malware to the servers and other infrastructure established by the United States, to include the date, time, and duration of the communication. The United States does not request and does not seek to obtain the contents of any communications, as defined in 18 U.S.C. § 2510(8).

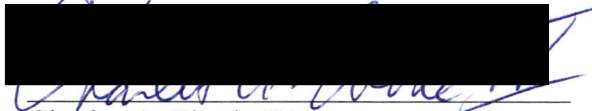
19. The United States further requests that the Court authorize the foregoing installation and use for a period of sixty days from the date of the Court's Order, pursuant to 18 U.S.C. § 3123(c)(1).

20. The United States further requests that this application and any resulting Order be sealed until further order of the Court, pursuant to 18 U.S.C. § 3123(d)(1).

21. The United States further requests that the Clerk of the Court provide the Department of Justice with certified copies of this application and Order, and provide copies of this Order to the FBI upon request.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on May 22, 2018.

A black rectangular redaction box covers the signature area. A blue ink signature is visible, partially obscured by the redaction and extending to the right.

Charles A. Eberle IV
Assistant United States Attorney
700 Grant Street, Suite 4000
Pittsburgh, PA 15241
Charles.Eberle@usdoj.gov
PA ID No. 80782